Blockchain Security in Safeshare

Safeshare Enhanced with Blockchain Technology

Cocoon Data has adapted Blockchain technology in SafeShare to provide industry-leading file security and an immutable history (cannot be changed) of all file activity over the life of the file.

Importantly, this high level of security is delivered as a SafeShare feature without the cost and complexity of deploying a HSM (Hardware Secure Module), which is the industry alternative.

The outcome is a solution that provides absolute confidence in the confidentiality, integrity and history of data from a highly trusted source (the blockchain).

How It Works

Blockchain and SkipChain technology is deployed in SafeShare to include file properties and additional security data in a blockchain that is stored across multiple nodes in the network.

The Chain has an unencrypted area for file activity history which needs to be viewable but secure from tampering, and an encrypted area for access permissions and encryption keys which need to be secured and unreadable.

Both the encrypted and unencrypted areas of the chain are protected according to their own business requirements, as outlined below.

Immutable File History (Unencrypted Area of the Chain)

The complete history of all file activity is stored on the chain as unencrypted data.

In this context, Cocoon Data's Blockchain solution provides:

1) Flexible Data Volume to Accommodate All History Logs

The chain data can be continually augmented with additional blocks required to store all file history logs with data volume that increases over the life of the file.

2) Security Against Tampering

A copy of each chain is duplicated on multiple nodes (computing elements) across the network. When a file is opened, the system compares the chain hash's (unique fingerprint of the contents of each chain) and immediately identifies if there is any difference to a duplicate copy stored on any other node. The outcome is that any tampering attempts will be alerted and blocked.

Encryption Key and Permissions Security (Encrypted Area of the Chain)

File access permissions and the file encryption keys are stored as encrypted data on the chain.

SkipChain technology is used to fragment the chain encryption key into multiple pieces, with each fragment stored on a different node making it virtually impossible to compromise.

This approach using Blockchain and SkipChain technology provides:

3) Industry-Leading Security for Encrypted File Properties Data

Security for file access permissions and the file encryption key data in the encrypted area of the chain is assured with a chain encryption key that is fragmented into multiple pieces, with each fragments stored in a different node.

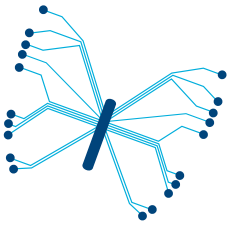
4) Multi-Layered Security for File Encryption Keys

Additional to the security for the chain encryption key as mentioned in 3) above, above, the actual files are additionally protected with combined symmetrical and asymmetrical encryption to deliver a multi-level encryption design.

The outcome is layers of encryption security with the first layer from blockchain technology, being the encrypted area of the chain, secured by an encryption key that is fragmented into pieces with each fragment stored on a different node as an industry leading security approach.

5) Affordability Compared to HSM Alternatives

This approach to security is available at a fraction of the cost of a HSM (Hardware Secure Module) which is generally considered as the alternative solution for highest encryption key security, but is complex, expensive and reliant on specific infrastructure.



Customer Benefits

Security Outcomes

1) Industry-Leading Security Against Unauthorised File Access

Industry-leading security against unauthorised access is assured with chain encrypted keys that are fragmented into pieces, with each piece saved on a different network node making it virtually impossible to compromise. This is in addition to the established multi-level file encryption.

2) Full Immutable and Secure Transaction History

A full immutable (cannot be changed) history of all file activity is stored on the Chain as viewable and secured with Blockchain technology.

3) Protection Against Tampering.

Protection against tampering or modifying the encryption keys, permissions or file activity logs is assured with duplicate copies of the Chain data stored across multiple nodes. Any inconsistency will be blocked and alerted as a (failed) tampering attempt.

Commercial Outcomes

4) Affordable High-Grade Encryption Key Protection.

This design provides the highest level of security for encryption keys and other file data without the formidable cost, complexity and infrastructure requirements of a HSM (Hardware Secure Module) which is generally considered as the alternative.

Customised Chain Data Options

5) Customised Chain Data Requirements

Our design capability allows us to integrate into the Chain any customer specific data requirements beyond the encryption keys, permissions and file activity logs that are included in the standard Cocoon Data product.

Examples might include special file classifications, identification certificates or more.